The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/16/2017

SUBJECT:
Multiple Vulnerabilities in Drupal Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Drupal core module, the most severe of which could allow for remote code execution. Drupal is an open source content management system (CMS) written in PHP. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Drupal Core versions prior to 8.2.7

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Drupal core modules, the most severe of which could result in remote code execution. Details of the vulnerabilities are as follows:

- A remote code execution exists by including development libraries that should be included in production deployments. (CVE-2017-6381)

- An access vulnerability exists in how the editor module checks access to inline private files. (CVE-2017-6377)
- A cross site request forgery vulnerability exists as some administrative paths do not include protection for CSRF. (CVE-2017-6379)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Drupal to vulnerable systems immediately after appropriate testing.
- Ensure no unauthorized systems changes have occurred before applying patches.
- Run all software as a non-privileged user to diminish effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Drupal:

https://www.drupal.org/SA-2017-001

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6377
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6379
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6381